Cybersecurity in Photovoltaic Plant Operations

Andy Walker,[1] Jal Desai,[1] Danish Saleem,[1]
and Thushara Gunda[2]

[1] *National Renewable Energy Laboratory*
[2] *Sandia National Laboratories*

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5D00-78755
March 2021

Cybersecurity in Photovoltaic Plant Operations

Andy Walker,[1] Jal Desai,[1] Danish Saleem,[1]
and Thushara Gunda[2]

[1] *National Renewable Energy Laboratory*
[2] *Sandia National Laboratories*

Suggested Citation
Walker, Andy, Jal Desai, Danish Saleem, and Thushara Gunda. 2021. *Cybersecurity in Photovoltaic Plant Operations*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-78755. https://www.nrel.gov/docs/fy21osti/78755.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5D00-78755
March 2021

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office Award Number 34172. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Acknowledgments

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office (SETO) Award Number 34172. The contributions and review of John Franzino, vice president of Grid Security at Grid SME, are gratefully acknowledged.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

List of Acronyms

CISA	Cybersecurity and Infrastructure Security Agency
DER	distributed energy resource
DERCF	Distributed Energy Resource Cybersecurity Framework
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
FIPS	Federal Information Processing Standards
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OT	operational technology
PV	photovoltaic
SCADA	supervisory control and data acquisition system
SP	Special Publication

Table of Contents

1 Introduction

Historically, the centralized power plants and vertically integrated utilities that comprised the electric grid had dedicated control systems and communications methods that allowed for remote operation and maintenance to occur without much regard or concern to cybersecurity risks. Photovoltaic (PV) systems, however, increasingly rely on common information technology (IT) computing and networking infrastructure as well as the Internet to perform all aspects of operation and maintenance, including but not limited to revenue metering, monitoring of condition, remote diagnostics, aggregation in virtual power plants, and control of grid support features such as curtailment and control of reactive power (Teymouri, Mehrizi-Sani, and Liu 2019). The transition of PV plant operations to an Internet-based world introduces many new security threats to the electric grid—including stealing or rerouting funds; denial of service; breaching confidential or proprietary information from a company, its customers, its suppliers; ransomware that denies operation of automated equipment for payment; and malicious control actions that could damage equipment and endanger personnel. Hackers intercept sensor control communications or use phishing and spoofing to obtain initial access and then use sophisticated means to escalate their access privileges for profit or to wreak havoc. Damage is not limited to interruption in operations or even plant equipment; it could extend to the electric grid, which was not originally designed for variable generation and bidirectional power flow.

The sophistication and resources available to an attacker have also evolved to include advanced and persistent threats. Unsophisticated attacks occur because a vulnerability exists and is taken advantage of by an attacker. Motivation for the attack is for entertainment or to be a nuisance. More sophisticated attackers seek to exploit your vulnerability motivated by monetary gain, the information has other value (reputation), or to cause damage. Corporate espionage is motivated by gaining access to your business plans, pricing, and intellectual property to gain a competitive edge through spying. Advanced and persistent threats can be either state-sponsored or through other sophisticated attackers with advanced capabilities and resources. They seek data and the capability to weaponize distributed energy resource (DER) systems. They can progress from initial infiltration to privilege escalation, to intelligence gathering, to data extraction, and to usurping communications and command/control actions. Vulnerabilities may be introduced in the supply chain, maliciously inserted into purchased software and hardware from network management software to software applications and down to the firmware and chipsets of devices. Stakeholders such as PV plant operators and utilities, providers of network equipment, standards making organizations, and others are addressing cybersecurity threats with a "Roadmap for PV System Cyber Security" (Johnson 2017) that share industry best practices, prioritize research topics; and advance developments in standards.

Rapid developments in IT exploit vulnerabilities in legacy systems but also can be used to make certain types of attack impossible. Legacy systems are vulnerable to certain types of attacks because of the rapidly advancing capability of IT exploits; however, these advances also include new ways to prevent attacks, based on commercial cloud security initiatives; mobile and "edge" computing; 5G telecommunications (which allow "slicing" of data); and quantum computing (which allows truly random number generation copy-proof communications, and fast machine learning of attack methods). This paper examines cybersecurity from the perspective of the PV

plant operator, compliance with adherence to standards, roles and responsibilities, best practices, and strategies to deal with an ever-evolving threat landscape.

1.1 Background and Context

Cybersecurity is central to issues of web use, data protection, and technology development. Beyond its most traditional applications, it could also be critical to instances of policy development, legal protection, health care, and education. The inherent interdisciplinary features of cybersecurity pose difficulty in defining it clearly. Craigen, Diakun-Thibault, and Purse (2014) agreed on the following definition: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Because web-based interactions are embedded in modern-day existence, researchers suggest the value of a shared doctrine of public security that outlines both the goals (policy creation) and means (regulatory measures) to uphold and protect cybersecurity (Mulligan and Schneider 2011).

Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Homeland Security's (DHS) newly created cybersecurity branch, highlights the importance of cybersecurity to national defense. Among its aims, DHS outlines strategies such as disruption to criminal use of the cyberspace, cyber incident response, and strengthened security of cyber activities (DHS 2019). Cybersecurity protections have been evolving for decades in instances of federal privacy legislation (i.e., Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act, Fair Credit Reporting Act), executive branch actions to ensure user privacy, and the U.S. Supreme Court's recent decision to extend constitutional rights to data held by third parties (Raul 2018).

The "roadmaps" for PV cybersecurity and Distributed Energy Resources cybersecurity engage stakeholders to share best practices, prioritize research and development needs, and steer new standards development (Johnson 2017, 2019). Cybersecurity is a topic that cuts across several agencies' domain and the roadmap effort is applauded by providing a high level of cooperation between stakeholder through a "working group" structure.

1.2 Current and Common Threats for Operators of Photovoltaic Plants

Cybersecurity incidents can take any form and some common types include: spearphishing to access an IT network and gain entry to the operational technology (OT) network; deploying software to encrypt data for ransom or to hamper operations; and accessing controllers that require no authentication for access or that communicate via commonly used ports and standard application layer protocols and modifying the control logic. Consequences of these kinds of incidents include a loss of visibility for human operators and resulting loss of operations (unavailability), loss of production, and loss of revenue (NSA and CISA 2020).

The first publicly reported cyberattack on a solar installation involved the exploitation of a known vulnerability in the firewall of commercial network software. In May 2019, a utility in the western United States reported to the U.S. Department of Energy (DOE) that they had been compromised by a denial-of-service cyberattack that targeted the company's firewall. The main cause of the attack was an unpatched Cisco firewall that gave hackers the ability to exploit the vulnerability and crash the device. This attack broke the connection between the utility's wind and solar power generation installations and caused a temporary disruption in its supervisory control and data acquisition (SCADA) systems, resulting in a series of 5-minute communications

outages between the independent power producer's grid control center in Utah and its generation facilities. The impacted generation totaled 500 MW, including a 106.3-MW PV project in California and an 80-MW wind power plant in Wyoming. The operator was not able to communicate with the plants for 12 hours, but the plants continued to operate autonomously, and no other consequences—such as a breach of data—were reported. This appears to be a crime of opportunity, with the hacker motivated by the vulnerable firewall rather than to attack this specific company (Sobczak 2017).[1] Later reports revealed that a Utah-based renewable energy provider, sPower, was the victim of this cyberattack (WETO 2020). It is said to be the first-of-its-kind attack to hit a renewable energy provider—and disconnecting a U.S. electric grid operator from its power generation station.

Cyberattacks against utilities are increasing in frequency and severity. North American Electric Reliability Corporation (NERC) President and Chief Executive Officer, Jim Robb, said that "the threat of a cyberattack is at an all-time high" (NERC 2019). According to the Global State of Information Security Survey 2015, the number of detected cyber incidents by power companies and electric utilities around the world had increased six times compared to the previous year. In Fiscal Year 2014, of the 245 total incidents reported to Industrial Control Systems Cyber Emergency Response Team, among all sectors, 55% involved advanced persistent threats or sophisticated actors, with 32% of incidents reported by energy sector companies (PWC 2014). Duke Energy, which serves nearly 8 million U.S. customers, reported more than 650 million attempted cyberattacks in 2017 alone (Diagle 2018)).

Attacks in other parts of the world indicate the vulnerabilities that exist in the cyber realm. For example, in 2016, cyberattacks on Kiev, Ukraine, left hundreds of thousands of civilians without power on several different occasions, representing the unrelenting threats posed to modern cybersecurity (Lee, Assante, and Conway 2016). Also, a cyber war by the "WannaCrypt" worm in May 2017 impacted 59,000 computers in nearly 100 countries, leaving negative economic and operational impacts in its wake (Venkatachary, Prasad, and Samikannu 2018). Despite few examples of infrastructural hacking in the United States, cybersecurity experts believe "we have been incredibly lucky that there hasn't been a catastrophic cyberattack against national infrastructure" (Smith 2018)—which suggests the issue is much less of an "if" and more of a "when."

A review of cyber-related entries within Sandia National Laboratories' PV Reliability Operations and Maintenance database (Gunda and Homan 2020) revealed additional insights. Operation-and-maintenance tickets discuss cybersecurity training, troubleshooting of firewall issues, and cybersecurity software updates; however, no reports of actual attacks were captured within the logs. This could be because cyber issues are treated separately from other physical maintenance and not reported in the computerized maintenance management systems. It is also possible that cyberattacks often go unrecognized or unreported.

[1] This article includes a link to the original DOE Office of Electricity Delivery and Energy Reliability *Electricity Emergency Incident and Disturbance Report*.

2 Challenges Faced by Photovoltaic Plant Operators in Implementing Cybersecurity

Challenges cited by PV plant operators include a lack of personnel with cybersecurity expertise to counter the threat. Also cited is a lack of cyber hygiene, such as weak passwords, outdated security software, and failure to frequently back up data. PV plants are most often unattended, making it costly and slow to get manual confirmation of a reported anomaly in a sensor reading or control setting.

Energy systems integration necessitates decentralized monitoring and control of distributed generation assets such as PV systems. Information must be passed around to provide ramp rate control, voltage regulation, fault identification and isolation, and configuration of circuits. Each component introduces a point of vulnerability: advanced meters, inverter controls, data acquisition and communications, building or facility energy management systems, weather monitoring, field sensors such as voltage measurements, actuators such as reclosers, and communications related to safety systems.

Overcoming these challenges involves plans that encompass this extended threat surface, training for staff, and certifications for security systems.

3 Cybersecurity Standards That Apply to Photovoltaic Plant Operations

The "Roadmap for PV Cyber Security" outlines a 5-year strategy for DOE, industry, and standards development organizations (Johnson 2018). The roadmap describes working group stakeholder engagement, research, and development priorities; best practices; and cybersecurity codes and standards to protect infrastructure, detect threats, recover from attacks, harden infrastructure, conduct self-evaluations, and practice good cyber hygiene and employee awareness (Johnson 2017). Similarly, the "certification procedure for cybersecurity of DERs," funded by DOE SETO, provides test cases that can be used by vendors, utilities, certification labs, government organizations, and industry partners to validate the cybersecurity posture of the existing and upcoming DERs.

Cybersecurity standards for solar PV are still at a very nascent stage, but a lot of work is already going on in this space. Broad working groups comprising industry, federal laboratories, universities, state energy officials, and standard development organizations are formed to develop consensus-based cybersecurity policies that could be applicable to a large number of systems and a nationally accredited certification standard for those functionalities (NARUC 2020; SunSpec Alliance 2020; SEPA 2020). Some of the well-established and most relevant standards to PV plant operations include:

- **DOE/DHS ES-C2M2**: Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
- **DOE/NIST/NERC Risk Management Process**: Electricity Subsector Cybersecurity Risk Management Process
- **NIST Cybersecurity Framework**
- **NIST SP 800-82 Revision 2**: Guide to Industrial Control Systems (ICS) Security
- **NIST Interagency/Internal Report 7628**: Guidelines for Smart Grid Cybersecurity
- **IEC 62351**: Power Systems Management and Associated Information Exchange - Data and Communications security
- **IEC 62443**: Security for Industrial Automation and Control Systems
- **IEEE C37.240-2014**: IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems
- **IEEE 1686**: Standard for Intelligent Electronic Devices Cyber Security Capabilities
- **NERC Reliability Guideline**: Cyber Intrusion Guide for System Operators
- **IEEE 1547.3**: IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems (currently under development)

In the United States, the National Institute of Standards and Technology (NIST) is one of the leading standards-making organization that also represents participation in other international standards. NIST published a *Framework for Improving Critical Infrastructure Cybersecurity* (NIST 2020) to consolidate many NIST information products into a sequence of identify, protect, detect, respond, and recover. NIST products include standards such as the Federal Information Processing Standards (FIPS) and Special Publications (SP), such as SP 500 Information Technology, SP 800 Computer Security, and SP 1800 Cybersecurity practice guides. NIST

interagency reports provide methods and data to standardize analysis. Much of this is general to all industrial control systems, but it can be readily adapted to the context of PV plant operation. Many NIST standards were developed with conventional utility operations in mind. They will continue to evolve and contemplate a higher level of distributed generation, the Internet of Things, and autonomous control.

Large PV power plants or large fleets of plants that provide power to the bulk electric system must comply with standards promulgated by NERC and enforced by the Federal Energy Regulatory Commission. This requires that an operator trains and certifies personnel in cybersecurity and critical infrastructure protection, emergency preparedness plans, services during and after disturbances, and communications between plants and grid operators. Specific critical infrastructure protection standards related to cybersecurity address categories of cyber systems and assets, security system management controls, configuration change management, personnel training and awareness, supply chain management, electronic security perimeters and access point protections, vulnerability assessments, incident response, incident reporting, and recovery plans. NERC standards apply to large plants delivering power to the high-voltage transmission system but will probably extend to smaller PV systems as distributed generation increases to the point that it can pose the same risks to the grid as the large plants currently do (Johnson 2019).

It is often said that standards prevent the worst but do not bring out the best. Because of the time it generally takes to develop and publish standards, compliance with standards alone is not enough to stay ahead of evolving threats. PV plant operators should proactively conduct cybersecurity evaluations, require all staff to practice cybersecurity hygiene and be diligent of internal threats, properly patching systems, address supply chain risks, and freely share information about attacks with others in the PV operations industry so that such attacks can be prevented.

4 Cybersecurity Response Plan for Photovoltaic Plant Operations

PV plant operators should have in place a plan to secure cyber systems and respond to attacks and resulting emergencies. The plan should be in place in advance of any attack so that the response to an information breach can be very quick. The plan should secure applications, operating systems, and communications protocols. The plan should be scalable with the enterprise and evolve with new information; consult with experts to conduct frequent security assessments and updates to plans. The following are items that a plan should include (Spencer 2019):

1. Definitions of cybersecurity incidents, such as inability to monitor or control versus loss of information.
2. Roles and responsibilities of each person involved in the response team; specify who the decision makers will be.
3. Contact information to call in case of an incident, including what each contact oversees within the company and external contacts, such as the utility company and law enforcement personnel.
4. A plan for which computers will need to be isolated from the network or locked and how data will be backed up.
5. Criteria for deciding what needs to be reported to emergency response, senior management, cybersecurity experts, legal counsel, suppliers, or insurance providers. Some notifications might be legal requirements if confidential information was stolen or disclosed.
6. Instructions on when to notify appropriate authorities. Contact your local police to file a report if there is a possibility that any personal information, intellectual property, or other sensitive information was stolen. Also consider contacting the local Federal Bureau of Investigation office, depending on the magnitude of the information security threat.

5 Best Practices and Additional Protective Steps to Ensure Photovoltaic Plant Cybersecurity

Insurance companies offer cybersecurity risk policies that cover damages caused by a cyberattack on IT and OT systems. Coverage might extend to damage to assets not actually owned by the insured, such as damage to a third-party substation or grid infrastructure that prevents the export of power. Coverage might also include the cost of a cybersecurity expert to assess the damage and exposure to risk, help in investigating and reporting the incident, loss of revenue caused by downtime, and any legal fees or fines caused by the cyberattack (Kenning 2018; Spencer 2019).

In 2020, a new initiative, the Cybersecurity Advisory Team for State Solar, was formed to bring together the National Association of State Energy Officials and the National Association of Regulatory Utility Commissioners, with additional support provided by the DOE Solar Energy Technologies Office (Stoker 2020). The initiative will leverage state, federal, and private-sector expertise on cybersecurity, grid, and PV to identify model solar-cybersecurity programs and actions for states to take in partnership with utilities and the solar industry.

A best practice is to conduct self-evaluations and/or assessments by expert consultants. Cybersecurity self-evaluations may use DHS US-CERT Cyber Security Evaluation Tool (CSET) (CISA 2021) or DOE/DHS Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (DOE 2014) to identify critical assets and devise plans to protect them (Johnson 2019). The Distributed Energy Resource Cybersecurity Framework (DERCF) provides U.S. federal government sites with a tool to assess the cybersecurity posture—or health—of their DER systems. This tool allows a user to assign roles to participants, answer a series of questions, and generate a report with recommendations.[2]

More robust research-and-development programs are needed to improve the effectiveness of cybersecurity guidelines while ensuring that they do not overburden system operators (Stamp 2017). In the meantime, utilities, aggregators, and equipment manufacturers could consider implementing and testing against appropriate elements of existing cybersecurity standards and guidelines as they become available. To start, they could align their cyber defenses to NIST's *Framework for Improving Critical Infrastructure Cybersecurity*. The following are several recommended security policies, procedures, and functionalities for PV plants and associated grid-edge devices that utilities, vendors, aggregators, and manufacturers can refer to:

1. Consider isolating internal and external communications of the PV systems from each other by setting up correct access through properly configured zones and subnets, maintaining air gaps between systems (i.e., restrict access internally from one system to another in case an intrusion cyberattack on one is successful), and separating security domains through the use of both signature and context-based firewalls, gateways, and secure ports. As an example, internal communications are those that could be used to communicate with DER controllers, SCADA systems, DER management systems, etc.,

[2] For more information, see https://dercf.nrel.gov/.

whereas external communications are those that could be used to communicate with the Internet, advanced metering infrastructure, cellular systems, etc.

2. Consider using authentication to ensure the identity of personnel, customers, vendors, and other systems and that these individuals have different privileges for accessing the DER monitoring and control systems. This also helps protect DERs from violating the least-privilege rule. For example, some enterprise networks require multiple means of authentication for access that range from requiring the password to sending a text message to your phone or an email with a unique and randomly generated passcode, or that require the user to enter biometric data, such as a fingerprint or a retinal scan; however, these all methods can be defeated if the verifier itself has been compromised or if the biometric image has fallen into the hands of a hacker. FIPS 140-2, *Security Requirements for Cryptographic Modules*, and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, provide independent, standards-based validation based on cryptography and security of the network to confirm both the authenticity of the request and the validation process; detection of intrusion by nonqualified personnel; detection of anomalous sensor readings or control signals; and reliable encryption of data transfers (Temin 2020; NIST 2001).
3. Consider using role-based access control (RBAC) and authentication for all communications, human-machine interface, and other interactions to authorize any read, write, create, or delete access to the stored data. Do not allow for overly permissive rules, and frequently remove unused or revoked access permissions.
4. Consider using Transport Layer Security (TLS) to ensure encryption, authentication, and data integrity. The latest version of Transport Layer Security is 1.3, and it should be standardized for distributed generation communications. This functionality helps protect the system against man-in-the middle, eavesdropping, and replay attacks. Also, consider using Simple Network Management Protocol or similar standards to monitor the health of communications networks and its components.
5. Consider using a Certificate Revocation List (CRL) to revoke expired and bad certificates that can no longer be used to authenticate the Transmission Control Protocol (TCP) session. This helps protect the system from data spoofing cyberattacks.
6. Consider adequate physical security such as video surveillance, badge-in access controls, fenced walls, door security and alarms, etc., to protect the hardware from malicious physical actions and to prevent unauthorized access that could cause serious data loss or damage to an enterprise or institution from man-made or natural events.
7. Consider using an antivirus software that has the capability to be frequently updated with new malware signatures and viruses. Provide long-term maintenance and scalability of security solutions, including ongoing patches.
8. Consider using application software patches and software data updates with rollback capabilities (if applicable). Having a rollback firmware capability protects the devices from malware that could be present inside the firmware updates or software files used by DER manufacturers or vendors to push the updates to the installed DER devices. This will also enable the DER device to revert to the previously known secure firmware and would limit any major impact on the electric grid.

9. Consider backing up data frequently by first running a malware scan, then encrypting the backup. Store this backup data in a physical location on a separate server, or in a secure cloud, in a way that it will not be lost by an attack on the original data (Spencer 2019). Also consider periodically testing your backup to make sure you can recover data.
10. Consider using effective password management methods and policies to ensure that connected devices could not be effortlessly undermined by brute force cyberattacks. Having effective password management policies helps protect the device— and eventually the overall distribution grid—from brute force credential attacks and least-privilege violations.
11. Consider using monitoring tools such as intrusion detection and/or prevention (IDS/IPS) that could monitor and examine network traffic flows to detect and prevent vulnerability exploits and to ensure that minimum due diligence to watch for cybersecurity incidents is being met regularly.
12. Consider using refined visualization to provide defense-in-depth architecture to help identify what is working well, where security incidents are occurring, and where system administrators can proactively address issues before they occur. Effective visualization could also refine human-based decisions and actions by presenting a format that is easier for humans to interpret instead of textual reports.
13. Consider using open-source tools that could provide effective logging for capturing important alerts, login attempts, irregular activities, etc. Logging is a key component of any security architecture. It involves the use of security devices that send alerts in addition to the operational technology devices that send logs. Also consider forwarding these captured alerts and logs to a centralized location on the network to enable network forensics against the network such as log analysis and audits.
14. Consider addressing supply chain management and insider threats to ensure that the smart devices—whether grid edge devices, DERs, behind or front of the meter—are reliable and secure, no matter where they are used, by creating a secure trust ecosystem for validating the supply chain risks of hardware software. Vulnerabilities could be built into hardware and software purchased commercially. NERC has introduced standard CIP-013-1—Cyber Security—Supply Chain Risk Management" to proactively address specific supply chain cyber risks with the aim of improving the reliability of bulk energy systems (NERC n.d.).
15. Consider consistent documentation within operation-and-maintenance logs to capture both the preventative and corrective actions taken to reduce and mitigate the risk of cyber vulnerabilities. This would allow industry-wide reviews of cyber-related activities at PV sites (both within and across portfolios).

6 Cost of Cybersecurity Measures in Operation of Photovoltaic Plants

Costs of measures taken to address cybersecurity include cybersecurity insurance, cybersecurity awareness training, antivirus software; monitoring of websites, servers, and domains; and data protection and backup. A cybersecurity assessment might be performed to identify threats and mitigations and to establish a long-term cybersecurity plan. These costs can vary widely. Free tools—such as CSET, ES C2M2 and DERCF, described in the previous section—can facilitate and reduce the cost of such a planning and assessment.

Insurance costs depend on specific coverages, data access, and network security of the insured as well as the claims history of the insured. Insurance premiums related to cybersecurity could be on the order of $1,500 per $1 million of coverage. It is often not the case that cybersecurity hazards are covered by conventional hazard and casualty insurance, which might cover physical hazards.

Training costs depend on the number of staff requiring for training and the training platform (in person or not). One advertised cybersecurity awareness training costs $1,000 for one-time training for up to 50 employees.

Antivirus software, backing up data, and monitoring are very inexpensive compared to the cost of recovering from an attack. Costs are often spread over a portfolio of PV plants, and they vary with scale and scope as well. Antivirus, anti-malware, and anti-phishing software might cost on the order of $1,500/year for continuous software updates. Monitoring of websites, portals, and domains might have minimal cost when spread over a large portfolio. Data protection and backup costs should be minimal when part of routine cloud backup.

A cybersecurity assessment with a professional consultant to study an organization's cybersecurity posture and threats and recommend a program to address all aspects of cybersecurity might cost on the order of $30,000 according to one practitioner and might be revised every year or every 5 years or so.

7 Conclusion

Threats evolve daily and dynamically, and cyber-physical systems are often created to mitigate threats in real time (Leszczyna 2018). Industry and regulators grasp the importance of cybersecurity in all aspects of PV plant operations. Updated software products and expert consultants offer some elements of protection, but elements are also assigned to every employee of a company—from the chief information officer to the person performing maintenance in the field. Standards offer a useful guide and help set expectations among parties, but PV plant operators can share and adopt best practices that not only comply with standards but also advance solutions to secure the energy system of the future, which will depend on increasing levels of communications and automation. Structured roadmaps for distributed energy cybersecurity help by providing a prioritization of required research and standards development (Johnson 2019).

References

Craigen, D., N. Diakun-Thibault, and R. Purse. 2014. "Defining Cybersecurity." *Technology Innovation Management Review* 4 (10): 13–21. http://doi.org/10.22215/timreview/835.

Cybersecurity& Infrastructure Security Agency (CISA). 2021. "Downloading and Installing CSET." Accessed January 12, 2021. https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET.

Daigle, R. 2020. "Duke Energy Hit by 650M Cyber Attempts to Breach Systems in 2017." *Bloomberg Law*, Environment and Energy Report, July 13, 2018. Accessed October 14, 2020. https://news.bloomberglaw.com/environment-and-energy/duke-energy-hit-by-650m-cyber-attempts-to-breach-systems-in-2017.

Gunda, T., and R. Homan. 2020. *Evaluation of Component Reliability in Photovoltaic Systems using Field Failure Statistics* (SAND2020-9231)." Albuquerque, NM: Sandia National Laboratories. https://doi.org/10.2172/1660804.

Johnson, J. 2017. *Roadmap for Photovoltaic Cyber Security* (SAND2017-13262). Albuquerque, NM: Sandia National Laboratories. https://sunspec.org/wp-content/uploads/2020/01/Roadmap-for-Photovoltaic-Cyber-Security-SAND2017-13262-4-10-2018.pdf.

———. 2018. *Roadmap for Distributed Energy Resources Cyber Security*. Albuquerque, NM: Sandia National Laboratories. Accessed January 12, 2021. https://www.researchgate.net/publication/322726557_Roadmap_for_Distributed_Energy_Resource_Cyber_Security.

Kenning, T. 2018. "Replication of Cyberattacks on Energy Sector a Threat to Renewables." *PV Tech*, September 7, 2018. Accessed October 10, 2020. https://www.pv-tech.org/news/replication-of-cyber-attacks-on-energy-sector-a-threat-to-renewables.

Lee, R., M. Assante, and T. Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case." Electricity Information Sharing and Analysis Center, March 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf accessed 1/7/2021.

Leszczyna, R. 2018. "A Review of Standards with Cybersecurity Requirements for Smart Grid." *Computers & Security* 77: 262–276. https://doi.org/10.1016/j.cose.2018.03.011.

Mulligan, D. K., and F. B. Schneider. 2011. "Doctrine for Cybersecurity." *Daedalus* 140 (4): 70–92. https://doi.org/10.1162/DAED_a_00116.

National Association of Regulatory Utility Commissioners (NARUC). 2020. "NASEO and NARUC Announce Initiative on Cybersecurity in Solar Projects: Cybersecurity Advisory Team for State Solar (CATSS)." June 18, 2020. https://www.naruc.org/about-naruc/press-releases/naseo-and-naruc-announce-initiative-on-cybersecurity-in-solar-projects-cybersecurity-advisory-team-for-state-solar-catss/.

National Institute for Standards and Technology (NIST). 2020. *Framework for Improving Critical Infrastructure Cybersecurity*. Accessed October 9, 2020. https://www.nist.gov/cyberframework.

———. 2001. FIPS 140-2: *Security Requirements for Cryptographic Modules*. NIST Computer Security Resource Center. https://csrc.nist.gov/publications/detail/fips/140/2/final.

National Security Agency (NSA) and Cybersecurity & Infrastructure Security Agency (CISA). 2020. "NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems" (U/OO/154383-20, PP-20-0622, July 2020 Rev 1.0). https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/1/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF.

North American Electric Reliability Corporation (NERC). n.d. "CIP-013-1 – Cyber Security - Supply Chain Risk Management." https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

———. 2019. Testimony of James B. Robb, President and Chief Executive Officer North American Electric Reliability Corporation, Before the House Committee on Energy and Commerce Subcommittee on Energy, "Keeping the Lights On: Addressing Cyber Threats to the Grid." July 12, 2019. Accessed January 7, 2021. https://www.nerc.com/news/testimony/Testimony%20and%20Speeches/House%20Energy%20and%20Commerce%20Cyber%20Hearing%20Testimony%207-12-19.pdf.

PWC. 2015. *Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015*. September 30, 2014. Accessed December 29, 2020. https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Raul, A. C. 2017. *The Privacy, Data Protection and Cybersecurity Law Review: 4th Edition*. London, United Kingdom: Law Business Research Ltd. https://thelawreviews.co.uk/.

Smart Electric Power Alliance (SEPA). 2020. "Explore SEPA's Working Groups." https://groups.sepapower.org/workinggroups/allworkinggroups/new-page.

Smith, D. C. 2018. "Enhancing Cybersecurity in the Energy Sector: A Critical Priority." *Journal of Energy & Natural Resources Law* 36 (4): 373–380. https://doi.org/10.1080/02646811.2018.1516362.

Sobczak, B. 2019. "First-of-a-Kind U.S. Grid Cyberattack Hit Wind, Solar." *E&E News*, October 31, 2019, Security. Accessed October 8, 2020. https://www.eenews.net/stories/1061421301.

Spencer, T. 2019. "How to Recover from a Cyber Attack." *Industry Week*, August 8, 2019. https://www.industryweek.com/sponsored/article/22028043/how-to-recover-from-a-cyber-attack accessed 10/10/2020.

Stamp, J. E. 2017. "Cyber Security for Renewable Energy." Presented at the 2012 Asia Pacific Clean Energy Summit and Expo, Honolulu, Hawaii, August 13–15, 2012. Accessed October 7, 2020. https://www.osti.gov/biblio/1116652%20accessed%2010/7/2020.

Stoker, L. 2020. "US Round-Up: New Solar Cybersecurity Initiative; Ex First Solar President Joints Tracker Firm." *PV Tech*, June 23, 2020. Accessed October 10, 2020. https://www.pv-tech.org/news/us-round-up-new-solar-cybersecurity-initiative-ex-first-solar-president-joi.

SunSpec Alliance. 2020. "SunSpec/Sandia DER Cybersecurity Work Group." https://sunspec.org/cybersecurity-work-group/.

Temin, T. 2020. "How to Choose the Right Multifactor Authentication Program." *Federal News Network*, October 9, 2020. Accessed October 12, 2020. https://federalnewsnetwork.com/cybersecurity/2020/10/3112884/.

Teymouri, A., A. Mehrizi-Sani, and C.-C. Liu. 2019. "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability." *Proceedings of IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*: 2,872–2,877. https://doi.org/10.1109/IECON.2018.8591583.

U.S. Department of Energy (DOE). 2014. *Cybersecurity Capability Maturity Model (C2M2)*. Washington, D.C. Accessed January 12, 2021. https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Wind Energy Technologies Office (WETO). 2019. *Roadmap for Wind Cybersecurity Roadmap*. Washington, D.C. Access January 7, 2021. https://www.energy.gov/sites/prod/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf.

U.S. Department of Homeland Security (DHS). 2019. "Cybersecurity Strategy." Accessed October 5, 2020. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf.

Venkatachary, S. K., J. Prasad, and R. Samikannu. 2018. "Cybersecurity and Cyber Terrorism—In Energy Sector—A Review." *Journal of Cyber Security Technology* 2 (3–4): 111–130.